UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,	:	
- against -	:	**MEMORANDUM DECISION & ORDER**
MARK NORDLICHT, DAVID LEVY, DANIEL SMALL, URI LANDESMAN, JOSEPH MANN, JOSEPH SANFILIPPO, and JEFFREY SHULSE,	:	16-cr-00640 (BMC)
Defendants.	:	

COGAN, District Judge.

This order addresses defendants'[1] motion to suppress materials seized during the search, pursuant to a search warrant (the "Warrant"), of the offices of Platinum Partners, L.P. ("Platinum"). For the reasons discussed below, defendants' motion is denied.

BACKGROUND

The Court presumes familiarity with the general background and procedural posture of the case. The following facts are relevant to the instant motion.

Platinum was a hedge fund, registered investment adviser, and fiduciary that held custody of investor funds. Pursuant to the Warrant issued by a Magistrate Judge, the Government conducted a search of Platinum's offices. During the search, the Government copied email inboxes from at least 18 individuals, seized materials from dozens of desks, filing cabinets, and

[1] Defendant Mark Nordlicht filed the suppression motion, which has been joined by defendants David Levy, Daniel Small, Uri Landesman, Joseph Mann, and Joseph SanFilippo (collectively, "defendants"). Jeffrey Shulse did not join the motion.

bookcases, and imaged at least 45 computers, hard drives, and other electronic devices.

The Warrant authorized seizure of materials falling into a particularized list of relevant categories, which included Platinum organizational charts; lists of employees and contractors and their roles and responsibilities; performance and valuation summaries for two Platinum funds; lists of investors and related information; communications with investors; communications to investors and auditors concerning Platinum's assets under management; records concerning Platinum's investments; policies, procedures, training materials and related documents; and bank records for Platinum entities. These categories of materials were tied to specified crimes, and were limited to those relevant to alleged violations after January 1, 2010. Additionally, the Warrant authorized the seizure of electronic devices that were either independently relevant or that contained relevant materials, along with access and use history information for those devices.

The Warrant was issued on the basis of a 22-page affidavit ("the Affidavit") that described a series of allegedly fraudulent schemes at Platinum.

At the time of the Government search, Platinum operated under a "Compliance Policies and Procedures Manual" (the "Compliance Manual"), which detailed, *inter alia*, maintenance of and access to physical and electronic records. Under the Investment Advisers Act, Platinum was required to obtain and maintain signed acknowledgements from employees that they had read and understood the Compliance Manual. See 17 C.F.R. 275.204-2(a)(12)(iii). For the purposes of this decision, significant excerpts of the Compliance Manual include:

- "The Firm shall preserve its books and records for the time periods provided in Rules 204-2(e) and (f) under the Advisers Act, which requires that all records be retained for at least six (6) years after last used . . ."

- "[T]he Advisers Act provides the SEC with authority to examine all books and records held by an advisor, not just those required to be maintained pursuant to Rule 204-2.

Specifically, Section 204 states that 'all records' of an investment adviser are 'subject at any time or from time to time, to reasonable periodic, special, or other examination . . .'

- "The Firm reminds its Employees that they have no expectation of privacy in their use of the Firm's systems or devices, and advises them to use discretion when using the Firm's e-mail system for business or personal matters and to minimize the use of the Firm's system for personal matters . . . . In using the Firm's email and computer systems, Employees waive any expectation of, or right to, privacy with regard to such use."

- "The Chief Compliance Officer shall examine the Firm's records on a periodic basis to ensure compliance with record keeping and retention requirements. The Chief Compliance Officer may periodically review Employee electronic communications for compliance with SEC rules and Firm policy. These measures may include accessing Employee electronic mailboxes to review individual messages and conducting keyword searches. The Firm has the right to monitor all activities involving its computers and the computer system. The Firm may, at its sole discretion, access any and all information on any computer or any portion of the computer system. The Firm's information system and all messages sent or retrieved electronically are the property of the Firm. All information created on, or with, Firm property belongs to the Firm and accordingly, Employees shall have no expectation of privacy in using email and/or IM services and the Firm's systems and devices. The Firm has no obligation to notify any Employee that his or her emails or IMs have been accessed and reviewed for any of the foregoing purposes. In certain circumstances, regulatory authorities may be given access to the Firm devices and computer system, or the information contained therein."

- "Because the Firm operates in a highly regulated industry, it may receive inquiries from a variety of governmental, regulatory or self-regulatory agencies or authorities such as the SEC, the CFTC, the U.S. Department of Treasury, the U.S. Department of Labor, the Department of Justice, state agencies and other local authorities."

The SEC's Office of Compliance Inspections and Enforcement ("OCIE") inspected Platinum's offices in 2014 and 2016, prior to the filing of the indictment in this case. All of the defendants were interviewed by OCIE staff in connection with these inspections. During the 2014 search, the OCIE requested "all emails" from a roughly two-year period for defendants Landesman, Nordlicht, Small, and Levy.

Only two defendants, Nordlicht and SanFilippo, submitted affidavits in support of the suppression motion, describing their work environment and their subjective expectation of privacy. Their affidavits established that Platinum's offices were not open to the public.

Additionally, Levy, Landesman, SanFilippo, and Small each had their own offices, and Mann had a workstation reserved for his private use. Platinum provided each defendant with a computer. Defendants were required to enter a unique password to access these computers. Platinum also provided each defendant with an individual email address, with access to the account also requiring a password.

At all relevant times, Nordlicht, as the holder of a majority stake in various Platinum entities, had control over Platinum's policies and decision-making. He stated that notwithstanding the above excerpts from the Compliance Manual, Platinum did not interpret the stated policies "as depriving [Platinum] personnel of privacy. Nordlicht stated that he was aware that "numerous Platinum personnel ([himself included]) used their Platinum-provided computers, email accounts, and other electronic data for personal and private purposes . . . and [Platinum] respected their privacy in doing so." He also recounts that, "in practice, [Platinum] did not routinely review personal or private electronic information in the computers, email accounts, or other electronic information of their personnel." He went on to state that he "never knowingly caused or permitted [Platinum] to review any personal or private electronic information in [his] Platinum-provided computer, email account, or other electronic data," and similarly "never knowingly caused or permitted [Platinum] to disclose voluntarily any personal or private electronic information from any Platinum personnel's Platinum-provided computer, email accounts, or other electronic data to [any law enforcement agency]."

Nordlicht and SanFilippo both stated that they expected that their Platinum-provided computer, email account, and other electronic information would not be reviewed by law enforcement absent proper legal authority to do so. SanFilippo stated, too, that he expected

tangible objects in his personal office to remain free from unwanted intrusion. Nordlicht did not include a similar statement in his affidavit.

DISCUSSION

I. Defendants' Expectations of Privacy

"A defendant seeking to suppress the fruits of a search by reason of a violation of the Fourth Amendment must show that he had a 'legitimate expectation of privacy' in the place searched." United States v. Hamilton, 538 F.3d 162, 167 (2d Cir. 2008). "This inquiry involves two distinct questions: first, whether the individual had a subjective expectation of privacy; and second, whether that expectation of privacy is one that society accepts as reasonable." Id. Determining if a defendant had a legitimate expectation of privacy is a "fact-specific" analysis. See United States v. Santiago, 950 F. Supp. 590, 597 (S.D.N.Y. 1996).

"In the workplace context, the Supreme Court has recognized that employees may have a reasonable expectation of privacy against intrusions by police." United States v. Yudong Zhu, 23 F. Supp. 3d 234, 237 (S.D.N.Y. 2014) (internal quotations omitted). "An expectation of privacy in commercial premises, however, is different from, and indeed less than, a similar expectation in an individual's home." Minnesota v. Carter, 525 U.S. 83, 90, 119 S. Ct. 469, 474, (1998). Defendants bear the burden of showing that they had a legitimate expectation of privacy in Platinum's offices. See Rawlings v. Kentucky, 448 U.S. 98, 104, 100 S. Ct. 2556, 2561 (1980).

Turning first to defendants' subjective expectations of privacy, "[i]t is well established that in order to challenge a search, a defendant must submit an affidavit from someone with personal knowledge demonstrating sufficient facts to show that he had a legally cognizable

privacy interest in the searched premises at the time of the search." United States v. Ruggiero, 824 F. Supp. 379, 391 (S.D.N.Y. 1993), aff'd sub nom. United States v. Aulicino, 44 F.3d 1102 (2d Cir. 1995). Only SanFilippo and Nordlicht submitted affidavits that arguably address this issue.

In his affidavit, SanFilippo stated that he had a private office at Platinum, and described occasionally using his desk, files, and computer for personal purposes. He also expressly stated that he expected his physical and digital personal files to remain private.

Nordlicht stated that he had a private office, which contained personal materials. He did not expressly state that he expected his personal materials to remain private, but the implication seems clear. He did, however, state that he expected his electronic information on Platinum devices to remain free from law enforcement review absent proper legal authority.

The remaining defendants did not submit affidavits. Nordlicht, however, in his affidavit described that Levy, Landesman, and Small each had their own offices, and that Mann had a workstation reserved for his private use. Nordlicht did not further describe their expectations of privacy as to their offices, but did state that they would be justified in having a similar expectation as he did with regard to their electronic information.

The Court is skeptical of whether the defendants who did not submit affidavits have adequately shown their subjective expectations of privacy in their electronic information and workplaces by relying on Nordlicht's affidavit. That affidavit gave what can charitably be described as cursory treatment to the privacy expectations of other defendants. See United States v. Fields, 113 F.3d 313, 320 (2d Cir. 1997) ("To contest the validity of a search, a defendant must demonstrate that he *himself* exhibited an actual subjective expectation of privacy in the area

searched."). Nevertheless, the Court will construe Nordlicht's affidavit as establishing the other defendants' subjective expectations of privacy.

Turning to whether defendants' expectations of privacy were objectively reasonable, the discussion below focuses first on defendants' expectation of privacy in their Platinum-issued electronic devices, which makes up the lion's share of the parties briefing, before turning to their expectation of privacy in their physical files. For the reasons discussed below, the Court holds that defendants did not have an objectively reasonable expectation of privacy in any use of Platinum-issued electronic devices, but did have a reasonable expectation of privacy in their physical offices.

As to electronic devices, neither the Supreme Court nor the Second Circuit appear to have directly addressed the specific issue here: if an employee has a reasonable expectation of privacy in electronic communications on private employer-provided electronic devices in the context of a police search.[2] However, the court in In re Asia Global Crossing, Ltd., 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005), developed a four factor test "to measure [an] employee's expectation of privacy in his computer files and e-mail." "In assessing an employee's reasonable expectation of privacy in a work computer or e-mail account, courts have increasingly turned to [the Asia Global test]." United States v. Finazzo, No. 10-CR-457, 2013 WL 619572, at *7 (E.D.N.Y. Feb. 19, 2013); see also In re Reserve Fund Sec. & Derivative Litig., 275 F.R.D. 154, 159-60 (S.D.N.Y. 2011) (the Asia Global test has been "widely adopted."). Although the Asia Global court applied the test in the context of evaluating if certain communications preserved

[2] The facts here are distinguishable from those in Leventhal v. Knapek, 266 F.3d 64 (2d Cir. 2001), a Second Circuit case addressing, *inter alia*, the question of a public employer's right to access an employee's computer. The Court there held that an employee "had a reasonable expectation of privacy in the contents of his office computer as the employer had neither a general practice of monitoring *nor a policy governing computer usage*." Curto v. Med. World Commc'ns, Inc., No. 03CV6327, 2006 WL 1318387, at *6 (E.D.N.Y. May 15, 2006) (emphasis added). Here, on the other hand, Platinum had a policy that explicitly governed its employees use of firm electronic devices.

attorney-client privilege, the court's analysis is broadly applicable, including to the Fourth Amendment context. In its privacy discussion, the Asia Global court cited repeatedly to Fourth Amendment analysis, and imposes no limiting language on situations where the test might be useful. At least one other court in this circuit has applied the Asia Global test in the suppression context. See Brown-Criscuolo v. Wolfe, 601 F. Supp. 2d 441, 449 (D. Conn. 2009).

The Asia Global test provides that when measuring an employee's expectation of privacy in his computer files and-email,

> [i]n general, a court should consider four factors: (1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?

In re Asia Glob. Crossing, Ltd., 322 B.R. at 257.

As to the first factor, although Platinum's Compliance Manual did not outright prohibit use of Platinum's electronic devices for personal purposes, it did advise employees to "minimize the use of the Firm's system for personal matters." Such an instruction suggests that Platinum's employees did not have an unfettered expectation of privacy. See Finazzo, 2013 WL 619572, at *8.[3] As to the second factor, the Compliance Manual expressly reserved a monitoring right: "[t]he Firm has the right to monitor all activities involving its computers and the computer system." "Where an employer reserves the right to access or inspect an employee's email or work computer, courts often find that the employee has no reasonable expectation of privacy." In re Reserve Fund Sec., 275 F.R.D. at 163 (applying the Asia Global test in the context of the marital communications privilege). In the face of this express policy, Nordlicht's statements that

[3] Defendants' citation to Curto, 2006 WL 1318387, at *6 is unavailing because the employee's computer at the center of the expectation of privacy dispute there was 1) used at home; and 2) not connected to the employer's network.

Platinum did not, in fact, routinely monitor employees' electronic activities is of minimal significance, because it always retained the right to do so, and its employees knew it. As to the third factor, Platinum was subject to SEC inspection "at any time," and this fact was detailed in the Compliance Manual. The manual also provided that "[i]n certain circumstances regulatory authorities may be given access to the Firm devices and computer system, or the information contained therein." The Compliance Manual goes so far as to point out (the obvious fact) that Platinum "operates in a highly regulated industry," and was accordingly subject to "inquiries" from a host of governmental authorities. What's more, the OCIE had previously requested "all emails" from Platinum, which would surely alert defendants (all of whom were interviewed by the OCIE) – if they were somehow, implausibly, not already on notice – that third parties could freely access their materials. Finally, as to the fourth factor, Platinum provided the Compliance Manual to all employees, as it was obligated to do by law.

Application of the Asia Global test, therefore, weighs heavily against finding that defendants had an objectively reasonable expectation of privacy in their Platinum-issued electronic devices.

Furthermore, a key fact independent of the Asia Global framework inclines strongly against finding that defendants had any reasonable expectation of privacy: in at least *three* instances, the Compliance Manual expressly alerted employees that they had no expectation of privacy when using Platinum's electronic devices. Significantly, one of these warnings immediately preceded (in the same sentence) the manual's instruction that employees should "minimize" their use of the devices for personal reasons, thereby foreclosing any argument that employees preserved some expectation of privacy as to only their personal use of Platinum's devices. The effect of this sentence is for Platinum to at once acknowledge that its employees

could make minimal personal use of its devices, but that when they did so, they would have no expectation of privacy. Defendants, therefore, had no objectively reasonable expectation of privacy in their use of any Platinum-issued electronic devices.[4]

As noted above, the bulk of the parties' arguments on the threshold issue of defendants' expectation of privacy focus squarely on the extent of any such expectation in their use of Platinum-issued electronic devices. However, to the limited extent that defendants suggest they had an objectively reasonable expectation of privacy in their physical offices and the physical files contained therein, they are correct. Such an expectation must, of course, be one "that society is prepared to consider reasonable," so defendants cannot credibly assert a privacy interest over areas beyond their private offices or personal workplaces. O'Connor v. Ortega, 480 U.S. 709, 715, 107 S. Ct. 1492, 1496 (1987); see e.g., Mancusi v. DeForte, 392 U.S. 364, 369, 88 S. Ct. 2120, 2124 (1968) ("In such a 'private' office, DeForte would have been entitled to expect that he would not be disturbed except by personal or business invitees, and that records would not be taken except with his permission or that of his union superiors."). Accordingly, defendants can challenge the validity of the Warrant, but only insofar as they claim it violated their privacy interests in their physical offices and physical files, including, for example, the contents of their "desk drawers and file cabinets." Hamilton, 538 F.3d at 168.

II. The Validity of the Search Warrant

Defendants argue that the Warrant was defective for three reasons. They claim that it violated the Fourth Amendment's particularity requirement, that it was unconstitutionally

[4] Insofar as defendants assert a privacy interest in their personal emails, as distinct from other personal electronic files, the Court is further skeptical of the viability of this claim for an independent reason: See United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) (Individuals may not "enjoy [] an expectation of privacy in transmissions over the Internet or e-mail that have already arrived at the recipient.").

overbroad, and that the Magistrate Judge who issued the Warrant did not have a "substantial basis" for finding probable cause.

Defendants argue that the Warrant violated the particularity requirement because, *inter alia*, "it authorized seizure of essentially every document involved in running Platinum's business," "without actual limitations or constraints," and that the property listed on the Warrant was "generally in lawful use in substantial quantities."

"The particularity requirement has three components. First, a warrant must identify the specific offense for which the police have established probable cause. Second, a warrant must describe the place to be searched. Third, the warrant must specify the items to be seized by their relation to designated crimes." United States v. Galpin, 720 F.3d 436, 445-46 (2d Cir. 2013) (internal citations and quotations omitted). "However, the standard for constitutional particularity requires only that a warrant be sufficiently specific to permit the rational exercise of judgment by the executing officers in selecting what items to seize." United States v. Dupree, 781 F. Supp. 2d 115, 150 (E.D.N.Y. 2011) (internal quotations and alterations omitted). "The nature of the crime, for example, may require a broad search." Id. at 149. "Where . . . complex financial crimes are alleged, a warrant properly provides more flexibility to the searching agents." Id.

The Warrant was sufficiently particular. First, it identified the specific offenses for which probable cause existed. Second, it described the location to be searched (Platinum's offices). Third, it narrowed the property to be seized to records, physical or electronic, post-dating January 2010 and relating exclusively to the designated crimes, "involving managers and employees of Platinum." The Warrant authorized seizure of additional access and user history

information for electronic devices. The Warrant, therefore, provided a temporal limitation, required that seized materials be tied to specific crimes, and listed custodians.

Even if, however, the Court were to hold – which it does not – that the Warrant were insufficiently particular, it would be valid under the "all-records exception." Under that exception, "[w]hen the criminal activity pervades that entire business, seizure of all records of the business is appropriate, and broad language used in warrants will not offend the particularity requirements." U.S. Postal Serv. v. C.E.C. Servs., 869 F.2d 184, 187 (2d Cir. 1989). An affidavit supporting a search warrant does not need to "set forth specific factual evidence demonstrating that every part of the enterprise in question is engaged in fraud" for the all-records exception to apply. United States v. Burke, 718 F. Supp. 1130, 1139-40 (S.D.N.Y. 1989). Instead, "the affidavit need contain only sufficient factual evidence of fraudulent activity from which a magistrate could infer that those activities are just the tip of the iceberg." Id. at 1140 (internal quotations omitted).

Here, the Affidavit supports the conclusion that the specific examples and indicia of fraudulent schemes that it detailed were just the "tip of the iceberg" of an extensive pattern of fraudulent conduct. Notably, the Affidavit stated that: 1) there was probable cause to believe that Platinum lied to investors about the performance of its funds and the value of assets therein; 2) Platinum's premier fund had improbably returned 17% on investments annually, without a single year with a negative return; 3) Platinum intended to use assets from one fund to repay others, rather than satisfy obligations, strongly suggesting that the use (or misuse) of Platinum's fund assets were inextricably intertwined; 4) there were alleged improprieties at two investment positions that together constituted roughly 50% of the holdings of Platinum's premier fund (the importance of the funds affected is significant in of itself, and also suggestive of more extensive

wrongdoing); 5) Platinum's managers and employees were widely involved in the alleged misconduct; and 6) their involvement extended to a host of Platinum's activities (including, for example, marketing, financing, and financial operations). Accordingly, the all-records exception provided independent justification for the Government's seizure of all Platinum records pertaining to its hedge fund business, which was credibly "permeated with fraud" at the time of the search.

Defendants argue that the warrant was overbroad "because the expansive categories of documents sought to be seized far exceed what would be reasonably necessary to investigate the allegations of fraud offered as probable cause for the search." Defendants claim that the Government could have conducted a narrower search that would still have left it able "to pursue its investigation without reaching every document involved in running Platinum's business."

A warrant is overbroad if it "provide[s] for the seizure of specific items for which there is no probable cause." United States v. Hernandez, No. 09 CR 625, 2010 WL 26544, at *8 (S.D.N.Y. Jan. 6, 2010). "The determination of whether there was probable cause sufficient to support the breadth of the warrants is based on a totality-of-the-circumstances analysis." Id. As to electronic property, "[p]reservation of the original medium or a complete mirror may therefore be necessary in order to safeguard the integrity of evidence that has been lawfully obtained or to authenticate it at trial." United States v. Ganias, 824 F.3d 199, 215 (2d Cir. 2016).

The Warrant was not impermissibly overbroad. The Warrant described a list of property to be seized that did not exceed the probable cause articulated in the supporting Affidavit. The Affidavit set forth enough facts to give rise to probable cause for the Magistrate Judge to believe that Platinum's managers and employees were engaged in schemes to defraud Platinum's investors, along with public bondholders, and that such fraud permeated Platinum's business.

The property authorized to be seized under the warrant was coextensive with the probable cause outlined in the Affidavit, and specified that the materials to be seized had to 1) post-date January 2010; 2) relate to the designated crimes; and 3) involve managers and employees of Platinum.

Defendants also argue that the Magistrate Judge lacked a substantial basis for finding probable cause, and that the issuance of the Warrant was therefore unconstitutional. A magistrate judge deciding whether to issue a warrant has to make a "practical, common-sense decision whether, given all the circumstances set forth in the Affidavit before him, including the veracity and basis of knowledge of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 238 (1983) (internal quotations omitted). Courts reviewing the issuance of a warrant "accord great deference to a judge's determination that probable cause exists, and [] resolve any doubt about the existence of probable cause in favor of upholding the warrant." United States v. Salameh, 152 F.3d 88, 113 (2d Cir. 1998) (internal quotations omitted). A reviewing court's duty "is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed." Gates, 462 U.S. at 14.

Defendants argue that four particular allegations in the supporting Affidavit were necessary to the Magistrate Judge's determination that probable cause existed, but that each allegation was fatally flawed, and that therefore the Warrant should not have issued. As discussed in the following paragraphs, each of the allegations in the Affidavit to which defendants point properly supported a finding of probable cause, and defendants' argument is unavailing.

First, defendants argue that the Affidavit improperly implied that Employee 1, a former officer of Black Elk (an oil company in which a Platinum fund was invested), stated or agreed

that Black Elk was fraudulently overvalued, although defendants claim that the Government's memoranda of the interview with Employee 1 said no such thing. Black Elk made up a substantial portion of Platinum's premier fund's total assets, so issues with its valuation, against Platinum's claims that the fund's assets remained steady through 2015, contributed to the inference that defendants engaged in fraud. But the Affidavit did not imply what defendants suggest it did. Instead, the Affidavit detailed that Employee 1 stated that Black Elk had no positive cash flow or net profit in 2013 or 2014, that Black Elk had few remaining assets following the sale of its "best assets," and that from 2012-2014, Black Elk was not generating sufficient revenue and could barely pay its bills. These statements reasonably casted doubt upon Platinum's consistent valuation of Black Elk, and supported an inference sufficient for a finding of probable cause. Defendants' reference to "well-established principles of finance" is unavailing at this stage, although they are free to raise it as a defense at trial.

Second, defendants argue that the Affidavit failed to establish probable cause that Platinum overvalued fund assets – specifically, Black Elk and Golden Gate (another oil company in which Platinum funds invested). The Affidavit pointed to falling oil prices, Black Elk's and Golden Gate's low production, and an industrial accident, to suggest that Platinum's consistent valuation of those assets, in the face of these issues, was fraudulent. As with their first argument, defendants are free to argue at trial that these facts are irrelevant considerations in the valuation of an oil company. But the Magistrate Judge was plainly not in error in considering them in finding probable cause to support the charge that defendants improperly overvalued fund assets. Furthermore, these facts were hardly the only allegations in the Affidavit giving rise to finding probable cause that a fraud was being perpetrated on Platinum's investors. For instance, the Affidavit also alleged that Platinum was selectively paying investor redemptions, improperly

intermingling fund assets, and fraudulently concealing from investors the truth about Platinum's liquidity.

Defendants' third and fourth arguments essentially take issue with the Magistrate Judge's weighting and interpretation of the evidence set forth in the Affidavit. For their third point, defendants claim that two statements in the Affidavit by an investor were not indicative of fraud: that a Platinum executive tried to get the investor to delay a redemption request because the next month would be a "big month," and that Platinum marketed shares with fewer redemption periods. For their fourth point, defendants claim that there was nothing odd about the fact of essentially identical monthly deposits and withdrawals, along with nearly equal starting and ending annual balances, in two of Platinum's funds. The Magistrate was, in the context of the rest of the Affidavit, entitled to draw inferences supporting probable cause from these allegations. As with the above points, defendants are also entitled to present defenses against these allegations at trial.

For the reasons discussed above, the Magistrate Judge had sufficient probable cause on which to issue the Warrant.

Because the Warrant was sufficiently particular, was not overbroad, and was issued on the basis of probable cause, it suffers from no defects that require suppression.

III. The Execution of the Search Warrant

Defendants also argue that the Government's execution of the Warrant requires suppression. They claim that the Government produced seized materials "without any review to determine whether the materials fell within the scope of the warrant," and that such production, "without taking steps to cull the documents not covered by the warrant[,] violates the Fourth Amendment reasonableness requirement." As examples, defendants point to 1) the

Government's production of documents outside the temporal limit of the Warrant; and 2) its production of sensitive personal documents and irrelevant information.

Defendants focus their arguments about the Government's execution of the Warrant squarely on the manner of its post-search, off-site review of seized electronic information – and not physical documents – and frame the Government's alleged failure to actually carry out that review as a breach of its "promise" to the Magistrate Judge that its "later off-site review of entire e*mail accounts, hard drives, and servers* . . . would be conducted 'consistent with the warrant.'" For instance, defendants state, "[c]onspicuously absent from the government's list [of how it conducted its review], however, is any effort whatsoever to exclude *electronic documents* that do not fall within the substantive bounds authorized by the magistrate judge;" "the government performed no technique – computer-assisted or otherwise – to determine whether the innumerable personal and irrelevant *emails* constituted evidenced described [in] the warrant;" "[t]he leeway the magistrate judge gave to collect Platinum's entire *server* was contingent on the government properly executing the warrant by searching for, identifying, and then excluding documents outside the specifically authorized categories;" and the Government was "on notice that when it collects a business's *electronic data*, it must execute the warrant by setting aside any materials not within the scope of the warrant within a reasonable time following the seizure."

It is axiomatic that a defendant alleging a Fourth Amendment violation "must show that he had a "legitimate expectation of privacy in the place searched." Hamilton, 538 F.3d at 167 (internal quotations omitted). Furthermore, a "defendant's Fourth Amendment rights are violated only when the challenged conduct invaded *his* legitimate expectation of privacy rather than that of a third party." United States v. Payner, 447 U.S. 727, 731, 100 S. Ct. 2439, 2444 (1980). "When a person has no privacy interest whatsoever in a particular container, place, or

conversation . . . Fourth Amendment analysis is straightforward – the person lacks standing to suppress the evidence obtained pursuant to an unlawful search of the place, or unlawful monitoring of the conversation." United States v. Karo, 468 U.S. 705, 725, 104 S. Ct. 3296, 3308–09 (1984).

Therefore, defendants cannot challenge the Government's execution of the Warrant as to electronic information. If defendants believe that the Government seized and produced *physical* documents from their offices that fall outside of the scope of the Warrant, defendants are to bring such documents to the Government's attention. Documents of a wholly personal nature that are not within the scope of the Warrant will be suppressed.

Defendants also argue that the Government's execution of the Warrant violated the Fifth Amendment's Due Process Clause. "The Supreme Court has suggested that in an extreme case, Government involvement in criminal activity might be so outrageous that due process principles would absolutely bar the Government from invoking judicial processes to obtain a conviction." United States v. Rahman, 189 F.3d 88, 131 (2d Cir. 1999) (internal quotations omitted). This is an onerous standard, and the Government's conduct falls well-short of what is required to assert a Fifth Amendment violation. As an initial matter, the material that the Government allegedly failed to review was seized pursuant to a warrant that 1) complied with the Fourth Amendment's particularity and overbreadth requirements; and 2) was based on probable cause. Furthermore, the Government has timely produced to defendants the seized materials, and those physical materials outside the scope of the Warrant in which defendants had a legitimate privacy interest will be suppressed. This state of affairs simply does not describe "governmental conduct, [that] standing alone, is so offensive that it "shocks the conscience . . . ." United States v. Chin, 934 F.2d 393, 398 (2d Cir. 1991).

Finally, "an evidentiary hearing on a motion to suppress ordinarily is required if the moving papers are sufficiently definite, specific, detailed, and nonconjectural to enable the court to conclude that contested issues of fact going to the validity of the search are in question." United States v. Watson, 404 F.3d 163, 167 (2d Cir. 2005) (internal quotations omitted). Although the parties vigorously disagree about the propriety of the Government's conduct, their dispute does not turn on contested facts, and the Court can reach the above conclusions without holding an evidentiary hearing.

CONCLUSION

For the reasons discussed above, defendants' motion is DENIED.

SO ORDERED.

Digitally signed by Brian M. Cogan

U.S.D.J.

Dated: Brooklyn, New York
February 2, 2018